

Dodatek č. 1

ke Smlouvě o poskytování služeb k zajištění činnosti pověřence pro ochranu osobních údajů a služeb v oblasti bezpečnosti informací IT

Číslo smlouvy: 2018/O/19

Poskytovatel: Tomáš Hofmeister
se sídlem: Hejnice 594, PSČ 463 62 Hejnice
IČ: 07153937
Bankovní spojení: ČSOB a.s.
Číslo účtu: 7215979/0300

a

Objednatel: KORID LK, spol. s r.o.
se sídlem: U Jezu 642/2a, PSČ 461 80, Liberec 2
spisová značka: C 21625 vedená u Krajského soudu v Ústí nad Labem
IČ, DIČ: 27267351, CZ27267351
zastoupený: Ing. Jiřím Zdražilem, jednatelem
Bankovní spojení: Komerční banka, a.s.
Číslo účtu: 35-5526710237/0100

shora uvedené smluvní strany uzavírají v souladu s § 1746 odst. 2 zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů, tento dodatek smlouvy:

Předmět dodatku

Předmětem dodatku č. 1 ke smlouvě je rozšíření rozsahu předmětu plnění smlouvy a změna níže uvedených ustanovení smlouvy, přičemž ostatní ustanovení smlouvy zůstávají beze změn.

Nové znění Čl. 1

Předmět smlouvy

(1) *Poskytovatel* (dále též „pověřenec“) se zavazuje vykonávat pro *Objednatele* činnost pověřence pro ochranu osobních údajů podle čl. 37 a násl. nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů).

(2) *Poskytovatel* se zavazuje oznámit dozorovému úřadu (Úřad pro ochranu osobních údajů) v souladu s článkem 37 odst. 7 obecného nařízení o ochraně osobních údajů kontaktní údaje jmenovaného pověřence, a to nejpozději do 25.5.2018 způsobem, který stanovil dozorový úřad. *Objednatel* se zavazuje pro toto oznámení zajistit pro *Poskytovatele* plnou moc správce osobních údajů.

(3) *Objednatel* je správcem osobních údajů ve smyslu čl. 4 odst. 7) obecného nařízení a je povinen ve smyslu čl. 37 odst. 1 písm. a) obecného nařízení jmenovat pověřence pro ochranu osobních údajů.

(4) *Objednatel* se zavazuje poskytovat pověřenci potřebnou součinnost při plnění závazku podle odstavce 1 předepsanou obecným nařízením o ochraně osobních údajů a dle ustanovení této smlouvy.

(5) *Poskytovatel* se dále zavazuje pro *Objednatele* zajišťovat konzultační služby a součinnost při zavádění interní dokumentace a následném dodržování zásad v oblasti systému řízení bezpečnosti informací tak, aby *Objednatel* řádně naplňoval případné právní povinnosti vyplývající z kybernetické bezpečnosti. Předmětem plnění není projektová činnost a řízení projektů *Objednatele*.

(6) *Objednatel* se zavazuje zajistit *Poskytovateli* potřebnou součinnost při plnění závazku podle odstavce 5, zejména při schvalování návrhů směřujících k zavedení interní dokumentace, dodržování zásad a provádění bezpečnostních opatření v oblasti systému řízení bezpečnosti informací.

Nové znění Čl. 2

Způsob plnění smlouvy

(1) Pověřenec vykonává svoji činnost v souladu s pokyny *Objednatele*. Tyto pokyny nesmí být v rozporu s postavením a úkoly pověřence podle čl. 37 obecného nařízení o ochraně osobních údajů.

(2) Pověřenec poskytne *Objednateli* kontaktní údaje fyzické osoby, která bude činnost pověřence fakticky vykonávat, a to v rozsahu: jméno a příjmení, telefonní číslo, adresa elektronické pošty. Tyto údaje slouží k zajištění dostupnosti pověřence a ke splnění informačních povinností ohledně těchto údajů vůči Úřadu pro ochranu osobních údajů a subjektům údajů a pro sestavení záznamů o činnostech zpracování.

(3) Pověřenec:

- a) poskytuje *Objednateli*, členům jeho orgánů a zaměstnancům informace a poradenství o jejich povinnostech podle obecného nařízení o ochraně osobních údajů a dalších předpisů v oblasti ochrany osobních údajů,
- b) monitoruje soulad s obecným nařízením o ochraně osobních údajů, dalšími právními předpisy a vnitřními předpisy a další dokumentací *Objednatele* v oblasti ochrany osobních údajů, včetně rozdělení odpovědnosti, zvyšování povědomí a odborné přípravy zaměstnanců zapojených do činností zpracování osobních údajů,
- c) poskytuje poradenství na požádání, pokud jde o posouzení vlivu na ochranu osobních údajů a monitorování jeho uplatňování podle čl. 35 obecného nařízení o ochraně osobních údajů,
- d) spolupracuje s Úřadem pro ochranu osobních údajů,
- e) působí jako kontaktní místo pro Úřad pro ochranu osobních údajů v záležitostech týkajících se zpracování, včetně předchozí konzultace podle čl. 36 obecného nařízení o ochraně osobních údajů, a případně vedení konzultací v jakékoli jiné věci, a
- f) působí jako kontaktní osoba *Objednatele* pro subjekty údajů v záležitostech souvisejících se zpracováním jejich osobních údajů a výkonem jejich práv podle obecného nařízení o ochraně osobních údajů.

(4) Pověřenec dále:

- a) sleduje vývoj právní úpravy, stanoviska Úřadu pro ochranu osobních údajů a orgánů Evropské unie a rozhodovací činnost soudů v oblasti ochrany osobních údajů a přiměřeným způsobem o těchto skutečnostech informuje *Objednatele*,
- b) sleduje vývoj technologií souvisejících s ochranou osobních údajů a přiměřeným způsobem o něm informuje *Objednatele*,
- c) posuzuje návrhy významných dokumentů *Objednatele* týkajících se ochrany osobních údajů,
- d) posuzuje soulad navrhovaných řešení v oblasti informačních a komunikačních technologií s pravidly ochrany osobních údajů,
- e) poskytuje součinnost při vyhodnocování podání subjektů údajů v záležitostech souvisejících se zpracováním jejich osobních údajů a výkonem jejich práv podle obecného nařízení o ochraně osobních údajů, přičemž *Objednatel* při vyřizování podání postupuje v souladu se svými vnitřními předpisy,
- f) posuzuje vedení záznamů o činnostech zpracování podle čl. 30 obecného nařízení o ochraně osobních údajů,
- g) spolupracuje při plnění povinností *Objednatele* hlásit porušení zabezpečení osobních údajů Úřadu pro ochranu osobních údajů (čl. 33 obecného nařízení o ochraně osobních údajů) a oznamovat porušení zabezpečení osobních údajů subjektům osobních údajů (čl. 34 obecného nařízení o ochraně osobních údajů).

(5) Do jednoho měsíce od uzavření této smlouvy a dále každoročně vždy do 31. ledna předloží pověřenec *Objednateli* ke schválení Plán kontrolních činností na příslušný kalendářní rok, který tvoří jako příloha č. 2 nedílnou součást této smlouvy.

(6) Rozsah plnění *Poskytovatele* v oblasti systému řízení bezpečnosti informací je uveden v příloze č. 4, která je nedílnou součástí této smlouvy.

Nové znění Čl. 4

Odměna a platební podmínky

(1) Za výkon činnosti pověřence ve smyslu této smlouvy náleží *Poskytovateli* měsíční odměna dle přílohy č. 1 této smlouvy.

(2) Odměna *Poskytovatele* zahrnuje výkon činností podle článku 2 odst. 3, 4, 5 a 6 této smlouvy včetně případných nákladů na cestovné.

(3) *Objednatel* se zavazuje výše sjednanou odměnu hradit měsíčně pozadu na základě *Poskytovatelem* vystavené faktury, kterou zasílá elektronicky *Objednateli* na adresu [REDACTED]

(4) Úhrada za příslušný měsíc je splatná do 10 (slovy deseti) dnů od obdržení faktury *Objednatelem*. V případě prodlení s platbou ze strany *Objednatele* je tento povinen uhradit *Poskytovateli* úrok z prodlení ve výši 0,5 % za každý den prodlení z nezaplacené částky.

Závěrečná ujednání

(1) Tento dodatek č. 1 smlouvy se vyhotovuje ve dvou stejnopisech.

V Liberci dne: 1.4.2021

Za *Poskytovatele*

Za *Objednatele*

.....

.....

Příloha č. 4 – Rozsah služeb v oblasti systému řízení bezpečnosti informací IT

Předmětem plnění je zajištění odborných profesních služeb informačních a komunikačních technologií (ICT) dle konkrétních potřeb *Objednatele* v oblasti problematiky systému řízení bezpečnosti informací IT (ISMS) pro *Objednatele*.

Zejména se jedná o tyto činnosti:

- a) spolupráce na činnostech modelu PDCA (Plan-Do-Check-Act) při zavádění ISMS pro *Objednatele*;
- b) monitoring aktuálních standardů a technických a technologických řešení v oblasti předmětné činnosti a návrhy jejich aplikace do prostředí *Objednatele*;
- c) provádění analýzy rizik a součinnost při řízení rizik ISMS v prostředí *Objednatele* s důrazem na zpracování a revize metodiky pro hodnocení aktiv a rizik, zpracování zpráv o hodnocení rizik a plánu zvládnání rizik;
- d) konzultace a podpora při řízení bezpečnosti informací IT dle platné legislativy (v souladu se zákonem o kybernetické bezpečnosti, vyhláškami, nařízeními vlády a další legislativou v oblasti bezpečnosti informací);
- e) podpora při aktualizaci systému řízení bezpečnosti informací IT a tvorbě příslušné dokumentace, tvorbě směrnic, politik, metodik a dalších interních předpisů *Objednatele*;
- f) návrhy a realizace jednotlivých analýz rizik IS a aplikací dle potřeb *Objednatele*;
- g) analýzy rizik spojených s přístupem třetích stran k prostředkům a informacím *Objednatele*;
- h) monitoring účinnosti bezpečnostních opatření a návrhy na zlepšení;
- i) tvorba a revize dokumentace bezpečnosti informací IT;
- j) konzultace při připomínkování přípravné a realizační dokumentace projektů a provozní dokumentace z pohledu předmětné služby;
- k) poskytování součinnosti v souladu s předmětnou službou při plánování, navrhování a řešení vývoje a změnách agendových systémů a technologických řešení v souladu s předmětnou službou;
- l) poskytování součinnosti, konzultací a informací dodavatelům ICT řešení v souladu s předmětnou službou v průběhu analýzy, návrhu řešení, realizace, akceptace a předávání do provozu;
- m) součinnost při poskytování vstupů do dokumentace veřejných zakázek, zejména požadavků vycházejících z předmětné služby a jejich souladu s platnou legislativou;
- n) ukládání dokumentace spojené s předmětnou činností v příslušné elektronické knihovně *Objednatele* (v úložišti disk.korid.cz);
- o) řízení se platnou legislativou a vnitřními předpisy *Objednatele* a plnění odborných úkolů v oblasti předmětné služby na vyžádání *Objednatelem* v rozsahu odsouhlaseném oběma smluvními stranami;
- p) činnosti nad rámec uvedeného rozsahu budou prováděny a účtovány na základě předem odsouhlasené nabídky oběma smluvními stranami.

Úroveň znalostí a certifikace pro tuto službu:

- q) znalost zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti) a další platné legislativy a návazných vyhlášek;
- r) znalost standardů a platné legislativy v oblasti ISMS (norma ISO/IEC 27001);
- s) znalost tvorby plánů kontinuity a havarijních postupů na odborné úrovni;
- t) znalost tvorby analýz v oblasti ISMS na odborné úrovni;
- u) znalost tvorby metodických předpisů ISMS na odborné úrovni;
- v) znalost testovacích a auditních procedur a metod z hlediska ISMS na odborné úrovni;
- w) znalost tvorby podkladů, výstupů a další dokumentace v českém jazyce na odborné úrovni a dobré komunikační schopnosti;
- x) platná certifikace Národního bezpečnostního úřadu (NBÚ) v rozsahu:
Osvědčení fyzické osoby na stupeň utajení „Důvěrné“ (číslo: NBÚ-124632)